

STAT

STAT

ILLEGIB

STAT

STAT

ILLEGIB

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

For Approval

FROM:

C/ISSD/OS

EXTENSION:

NO.

DATE:

20 July 87

TO: (Circulate to all offices, agencies, and buildings)

DATE

OFFICER'S INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across columns after each comment.)

RECEIVED

FORWARDED

C/ISSG/OS

C/SS/OD&E

C/SS/OL

EO

20 JUL 1987

2007

R

9.

C/ISSD

10.

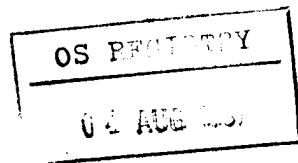
11.

12.

13.

14.

15.



20 JUL 1987

MEMORANDUM FOR: Director of Security

VIA: Chief, Security Staff, Office of Development
and Engineering
Chief, Security Staff, Office of Logistics
Chief, Information Security Group

25X1 FROM:
Chief, Information Systems Security Division
Office of Security

25X1 SUBJECT: Request for Approval

25X1 REFERENCES: A. "Security Requirements for Contractor
Automated Information Systems Processing
Sensitive Compartmented Information"
25X1 B. "Security Requirements for Contractor
Automated Information Systems Processing
COLLATERAL Information"

25X1 1. The Information Systems Security Division (ISSD)
requests your approval to distribute an updated "Security
Requirements for Contractor Automated Information Systems
Processing Sensitive Compartmented Information" (SCIREQ004) and
"Security Requirements for Contractor Automated Information
Systems Processing COLLATERAL Information" (COLREQ003).

25X1 2. The last issuance of security requirements for Agency
contractors performing SCI data processing is dated August
1984, and the last issuance of security requirements for Agency
contractors processing COLLATERAL information is dated
September 1983. Both of these documents urgently require
updating.

25X1
~~SECRET~~

3. The attached requirements documents are the result of a major effort to update the 1984 and 1983 sets of requirements. These documents:

a. Are pursuant to Director of Central Intelligence Directive (DCID) 1/16 and incorporate portions of DCID 1/7, 1/14, 1/19 and NFIB/NFIC-9.1/47 relative to the industrial computer security environment.

b. Are based on the ISSD document, "Minimum Security Standards for Automated Data Processing Systems", which provides guidance for determining the degree of trust needed for future Agency systems.

c. Specify automated information system (AIS)-related responsibilities for the contractor, the assigned Agency Information Systems Security Officer (ISSO), the assigned Agency Contracting Officer's Security Representative (COSR), and the assigned Agency Communications Security (COMSEC) officer.

d. Specify a set of required documentation which the contractor must prepare and submit, for approval, prior to processing Agency information.

e. Incorporate all existing requirements and policies pertaining to the industrial computer security environment.

f. Update the requirements pertaining to system standards and magnetic media sanitization, and for preparation of the AIS Security Program Plan and AIS Certification Test Plan.

g. Introduce new requirements pertaining to network security and configuration management.

4. As stated in previous requirements documents, these documents clearly state that the contractor's AIS Security Program Plan shall be based on the type, size, and configuration of the various elements of

the individual contractor's environment, and that ISSD, acting for the Agency, will determine (negotiate), in close coordination with the COSR, COTR, and contractor-designated Automated Information Systems Security Representative (AISSR), the complete spectrum of security controls for each individual AIS.

Attachment

CONCUR:

Chief, Information Security Group

Date

21 July 87

Chief, Security Staff, Office of Development and Engineering

Date

21 July 87

Chief, Security Staff, Office of Logistics

Date

21 July 87

APPROVED:

Director of Security

Date

7/31/87